Mapping Cybercrime Laws and Violations of Digital Rights in the Gulf and Neighbouring Countries

Gulf Centre for Human Rights

June 2018

Table of Contents

I. Executive Summary: Mapping Cybercrime Laws and Violations of Digital Rights in the Gulf and neighbouring Countries 3

II. Background on cybercrime legislation in the region 4

III. Cybercrime laws in the Gulf Countries: Penalisation and Prosecution of Online freedom of expression, opinion and thought 5

1. Bahrain 5

2. Kuwait 7

3. Oman 9

4. Qatar 11

5. Saudi Arabia 12

6. United Arab Emirates 14

IV. Cybercrime laws in neighbouring countries: Reinforcing repression and violations 15

1. Jordan 15

2. Syria 17

3. Lebanon 19

V. Conclusion 21

VI. Recommendations 23

I. Executive Summary: Mapping Cybercrime Laws and Violations of Digital Rights in the Gulf and neighbouring Countries

During the week before the arrest and detention of the prominent human rights defender, **Ahmed Mansoor**, the United Arab Emirates (UAE) mandated the creation of Federal Public Prosecution for Cybercrimes on 17 March 2017. A year later, on 25 March 2018, the Syrian government has mandated a specialised prosecution unit upon Presidential decree 9/2018. To establish specialised courts for cybercrimes in two countries in the region, targeting human rights defenders, is an alarming sign and a direct threat to digital rights and online freedoms of expression, thought, opinion and press. Digital rights and freedoms have been severely compromised by national cybercrime legislation and prosecution, and now judicially. The general trend for prosecution was that digital rights and freedoms were penalised and ruled as "cybercrime" cases delegated to general courts. Verdicts in these cases have been either based on an existing penal code where cybercrime laws are absent, in the process of being drafted, or under the penal code and a cybercrime law.

Prior to the UAE and Syrian decisions, the region has witnessed an interest in creating national cybercrime legislation and specialised police departments. These departments are primarily concerned with monitoring, filtering and prosecuting netizens, human rights defenders, journalists and bloggers for exercising their online freedom of expression, thought, opinion and press. Some countries have not developed their cybercrime laws yet, but indeed prosecute the aforementioned targets through the efforts of police cybercrime departments. In these cases, individuals are charged for threatening national security, defamation of religion, etc.

The rhetoric and justification for criminalising online content critical of governments in national cybercrime laws appear to stem from the 2010 Arab Convention on Combating Cybercrime (ACCC). The ACCC reiterates some articles in the region's earliest cybercrime legislations, namely those of the UAE and Saudi Arabia, which prosecute any cyberactivity deemed as a "threat to national security, unity and economy and religion."

This report presents a snapshot of the most problematic aspects of national cybercrime laws across the Gulf countries, Jordan, Syria, and Lebanon. Unless otherwise cited, the report is based on GCHR research and cases of human rights defenders.

In addition to surveying articles of the law and cases of prosecution, this report borrows on two main indicators to highlight the correlation between repressive cybercrime laws and the targeting of civic cyberactivism and the violation of digital rights. These indicators are: the CIVICUS Monitor Rating[1] and Freedom House's Internet Freedom Scores[2]. The CIVICUS Monitor, for which GCHR is the research partner in the Gulf region and neighbouring countries, classifies the status of civic space based on a government's efforts to foster or close civic space. The Internet Freedom Score[3] is more specific to the status of digital rights and access on a scale from 1 to 100 where 100 stands for "least free."

[1] https://monitor.civicus.org/

[2] Kuwait, Oman and Qatar are not covered in Freedom House's Freedom on the Net Report, hence, no Internet Freedom Score available.

[3] Internet Freedom Score cited in this report is for 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2017

With the insight of these two indicators, this report demonstrates that lack of online freedom and respect for digital rights is key to understanding and reporting on governments' wider crackdown of civic space and activism. Indeed, governments across the region keep a close eye on those who are active in cyberspace, promoting digital rights and civic activism, to target them or use their activism to justify reprisals.

II. Background on cybercrime legislation in the region

Though the Arab Spring is widely cited as the tipping point for increased repression on activism for political and social reform and change, Arab governments across the region have collaborated to formally restrict cyberspace even before the Arab Spring. Cybercrime legislations have been an endeavour launched as early as 2006 in the region. The first cybercrime law came from the UAE in 2006, followed by Saudi Arabia, and Jordan in 2007 and 2010 respectively.

A more concrete collaborative effort was evident in the creation of the ACCC[4] in late 2010 by the League of Arab States. The ACCC criminalises the use of Information Communications Technology (ICTs) to exercise freedom of expression and opinion. The ACCC, which further strengthens governments' cybercontrol, grounds the principle of sovereignty of the state in cyberspace, prosecution of thoughts and opinions that threatens national security, economy, morals, and order, and prosecution of online activity that violates other laws which criminalise and penalise non-cyberrelated offences i.e. laws for offline offences apply online. More distressingly, Article 21 of the ACCC advises party-states to increase and harshen the penalty of offline crimes committed over the Internet. Most of the member states signed the ACCC (expect for Lebanon, Djibouti, Comoro Islands, and Somalia) as it was proposed in December 2010. The ACCC only came into force in November 2014 after Egypt signed to validate it, along with six other states. The seven signatory states are: Kuwait, Qatar, Palestine, UAE, Jordan, Sudan, and Egypt.

One of the main contributions of the ACCC in the drafting of national cybercrime legislation is the definition it sets for technical terms. In this regard, the ACCC defines a "website" as any accessible page through a specific address over the web. In this respect, it puts all online content and data, of individuals and organisations, public and private, under scrutiny. The subsequent laws copy this definition and accordingly prosecute digital rights.

On a different level, Internet shutdowns were not exclusive to the Egyptian government in 2011 to compromise the mobilisation of protestors, but were preceded by the Syrian government's blockade on Facebook in 2007 after they became alarmed by increasing political opposition assembly in cyberspace. The most critical aspect of this form of repression is to disallow netizens, activists, bloggers and journalists the ability to communicate amongst themselves, their communities and others who do not live in the same country. Such has been translated into judicial ordeals which prosecuted individuals for damaging the state's reputation and/or communicating with foreign entities. Although this report does not investigate Internet shutdowns, it is important to highlight the different interventions introduced by governments in order to repress human rights writ large.

[4] Arabic text of the Convention can be accessed through the following link: https://bit.ly/2HPPKJy.

III. Cybercrime laws in the Gulf Countries: Penalisation and Prosecution of Online freedom of expression, opinion and thought

1. Bahrain

Bahrain passed its national cybercrime legislation under Law 60 of 2014 on Information Technology Crimes. The Law is complemented by other bodies of law including: media regulation, telecommunications and anti-terrorism laws. The Information Technology Crimes Law does not in itself criminalise online freedom of thought, opinion and expression but allows the prosecution of free expression as it complements Media Regulation Law of 2002[5]. Article 1 of the Law recognises the right to thought and expression bound by two conditions: respect for Islamic pillars and not inciting sectarianism. Freedom of press is subjected to these restrictions as well. Article 70 of the Media Regulation Law penalises content that is ruled to ridicule national security, as "fake news," or critical of public figures and states with which Bahrain has strong diplomatic ties.

Moreover, the Bahraini Cybercrime Directorate classifies "fake news" as one of the triggers for threatening national security and the economy. On the Internet Freedom Score, the score is 71/100 with violations of user rights and limits on content being the most problematic aspect, as demonstrated by the aforementioned regulations. Notably, Bahrain's score increased from 62 in 2011 and gravitated between 71 and 74 across the following six years.

Bahrain is classified as "closed" on the CIVICUS Monitor Rating, which cites harsh and systemic targeting through enforced disappearance, detention and torture. This particularly highlights the threats facing human rights defenders, activists and journalists if they are prosecuted by the repressive Media Law and Cybercrime Directorate's standards which criminalise freedom of speech, expression and opinion. The prime concern for the Cybercrime Directorate at the moment is content on social media. To this end, the government purchased Internet censorship technology from the Canadian company Netsweeper in January 2016. The technology purchased allows the Bahraini government to block access to a wide range of websites that host content pertaining to different aspects judged to challenge the government e.g. human rights, freedom of religion, and news published by media outlets that are critical of the Bahraini government[6].

Prominent human rights defender **Nabeel Rajab**, co-founder of GCHR and President of the Bahrain Center for Human Rights, was detained and arrested repeatedly for his tweets. Arrested on 01 October 2014 and on 20 January 2015, Rajab was sentenced to six years in prison for tweets that were critical of the Ministry of Interior's ideological indoctrination which he asserted foster terrorism. Rajab was arrested again on 02 April 2015 for tweeting about torture in Jaw prison where his tweets were classified as "fake news," and for pointing put the atrocities of the Saudi-led airstrikes on Yemen which were deemed as "offending a foreign country" under the Bahraini Criminal Code. Currently, Rajab is serving two prison sentences totalling seven years for media interviews about Bahrain, and for tweets about Jaw prison and denouncing the war in Yemen, which is an outright violation of his exercise of freedom of opinion, thought and expression.

---

[5] Arabic text of Media Regulation Law 47 of 2002 is available at http://www.mia.gov.bh/ar/Media-in-Bahrain/Pages/Media-Regulation-Law-in-Bahrain.aspx.

[6] Local and regional human rights organisations' websites were blocked such as the Bahrain Center for Human Rights and the Arabic Network for Human Rights Information.

The Bahraini government's targeting and clampdown on digital freedoms is not only directed at human rights defenders and journalists. In fact, society at large is under extreme scrutiny for their activities, interactions and communications over the Internet.

Accordingly, the surge in Bahrain's Internet Freedom Score ranking starting in 2011 can be explained by the realisation of the challenge posed by strong cyberactivism strength to challenge government policies. Twitter has been the platform for unveiling the injustice and violations of human rights committed in Bahrain. Following the events of February 14, Bahraini netizens were informed about the escalating levels of repression. The unfair trial and inhumane prison conditions of the twenty medics sentenced to between five and fifteen years in prison for assisting victims in the protests were documented via Twitter.

The government was not bothered by persistent calls to investigate torture in prison and continued prosecution on the pretences of prosecuting those who spread false information. This further pushed open the space for cyberactivism as it proved effective in highlighting these violations. On a different note, the Bahraini "tweep," Nazrad[7], documented the grotesque prison conditions, ill-treatment and torture he experienced in Al-Naim jail. Nazrad was imprisoned for tweets he posted on his personal account.

In 2014, women's rights defender **Ghada Jamsheer**, was arrested and charged with defamation as she tweeted about corruption in King Hamad Hospital. Jamsheer spent a compound prison sentence on numerous charges in September 2014 and again from August to December 2016 and was only released from prison to carry out community service for the remainder of her prison sentence (four months).

In order to highlight that repression in Bahrain is of a large-scale and writ-large antagonism, a campaign was launched in November 2011 by netizens in order to pressure the government to free those who have been imprisoned for their engagement with the February 14 movement. This campaign was concerned with military personnel who were tried in military courts for defying orders to shoot protestors, an expression of resistance similar to that of the medics.

The reach of violations and repression extended to more netizens. The former Member of Parliament, **Khalid Abdulaal**, was sentenced to one year in prison after the Cybercrime Directorate filed a case against him for tweets that fuel sectarianism and insult the Ministry of Interior when his tweets protested the use of torture by the Ministry. Sports journalist and YouTube Vlogger **Faisal Hayyat** was harassed repeatedly in 2016. Being one of the detainees in 2011, Hayyat used social media to voice and protest the torture he was under during his three-month imprisonment in a letter to the government (posted on Facebook) on 01 October 2016. Hayyat was arrested on 09 October 2016 to answer to this letter, and later sentenced on 29 November 2016 to three months in prison for defaming religion.

[7] "Nazrad" is the pseudonym under which the netizen used to share his 66 prison conditions in Al-Naim jail. The account has been deleted but the story coverage is available on GlobalVoices.

A new form of intimation appeared in May 2017, when blogger **Hassan Al-Sharqi** was summoned by the National Security Agency (NSA) and later declared in a tweet on 28 May that he will stop tweeting. Reports confirmed that he was insulted, beaten and ordered by a security officer to stop his online activities.

On 18 July 2017, the Public Prosecution ordered the six-month detention[8] of **Ebtisam Al-Saegh**, the monitoring and documentation officer of Salam for Democracy and Human Rights. She was arrested on 03 July 2017 during a raid by the NSA on her home and Al-Saegh to be incarcerated for six months pending investigation under the anti-terrorism law. On 22 October 2017, she was released from prison pending trial. Previously, while detained at Muharraq police station on 27 May 2017, Al-Saegh was tortured and sexually abused.

In 2017, the security authorities arrested and tortured many human rights defenders and then released them after forcing them to stop their human rights activities. Other people who were interrogated at Muharraq police station subsequently renounced their work on Twitter and stopped tweeting. Only Al-Saegh strongly condemned these illegal practices, describing them on Twitter as a "crime against humanity."

2. Kuwait

Prior to the creation of Kuwait's national cybercrime law, Law 37/2014 on the Creation of Communication and Information Technology Regulatory Authority (CITRA)[9] criminalised online content. Article 70 criminalises the misuse of Information Communication Technology (ICT) under penalty of a prison sentence and fine. Such misuses include: producing and disseminating content that is defamatory and against public ethics and mores and faking news. The purpose of creating CITRA, as detailed in Article 3 of the Law, only specifies that it assists respective authorities in undertaking the necessary technical measures to collect digital forensics and evidence for the prosecution of ICT misuses that are against Kuwaiti laws and a threat to public order and principles. The Articles of the Law however indicate that CITRA's authority is in fact policing rather than confined to this role of providing technical assistance. In effect, this further strengthens the grip on digital rights and cyberactvisim to prosecute human rights defenders, journalists, bloggers and netizens at large under the pretexts of preserving public order and fighting terror arising from the spread of fake news.

On 06 January 2015, ex-lawmaker **Saleh Al-Mulla** was summoned and detained for ten days in investigation over his tweets. These tweets resulted in charges of "insulting the Emir of Kuwait, the President of Egypt and endangering bilateral relations." The tweets in question were aligned with Al-Mulla's right to freedom of opinion and expression as it was critical of the government's decision.

[8] https://www.gc4hr.org/news/view/1713

[9] Available in Arabic at https://citra.gov.kw/sites/ar/LawofCITRA/%D9%82%D8%A7%D9%86%D9%88%D9%86%2037%20%D9%84%D8%B3%D9%86%D9%87%202014.pdf

Approved by the National Assembly on 16 June 2015 and coming into force in January 2016, the Kuwaiti Law 63/2015 on Combating Cybercrimes[10] states that it builds on the ACCC based on ratification in 2013. Accordingly, Articles 4, 6 and 7 of the ACCC are observed by the Law and hence leaving all online content to be prosecuted. Article 4 penalises creating websites that may contain/implicate content that prejudices public morality with a two-year prison sentence, a fine that is not less than US$6600 and does not exceed $16,500, or either. Article 6 and 7 subjugates online content to the mandates of Articles 27 and 28 of the Press and Publishing Law of 1960 which in turn penalises content that instigate "overthrowing the regime" or "aims at destroying the basic statutes of Kuwait through illegal means" with a sentence of ten-years' imprisonment.

GCHR and four other organisations signed a statement on 21 January 2016 after the Cybercrime Law was enacted, calling on the government of Kuwait to repeal these problematic Articles in both the Combating Cybercrime Law and the Press and Publication Law in order to prevent the prosecution of human rights defenders and online activists. In spite of these calls, the government issued the Electronic Media Law 8/2016[11] on 07 February 2016 which assumes governmental authority over establishing websites and electronic media by registration and through approval of the authorities.

The Public Prosecution issued an order to imprison the blogger, **Sara Al-Drees**, on 22 September 2016. She was charged for violations according to the Cybercrimes Law by allegedly defaming the Emir of Kuwait and misuse of her phone to tweet. Al-Drees was then under a travel ban after she was released from prison on a bail of US$1656.

Local newspapers reported on a draft law in January 2018 which aims to regulate content posted to Twitter. The bill is aimed at criminalising speech on social media platforms and other communication applications as the existing Electronic Media Law does not scrutinise this content. CITRA is as well not concerned with social media in particular. The same trend unfolded in other Gulf countries' draft cybercrime legislation, listing vaguely worded crimes which leaves it open to prosecution to rule any content that does not appeal to the authorities as a "means of annoyance and aggression against others."

According to the CIVICUS Monitor Rating, Kuwait's civic space is "obstructed " which makes it less repressive than other Gulf countries. This however does not negate that Kuwait followed suit of other Gulf countries to crack down on online dissidence and devised the legal framework and developed the rhetoric to justify this crackdown. Nonetheless, Kuwait has the lowest Internet penetration rate in Gulf countries at 82.1 percent, but the government is indeed wary of this rate. Hence, practiced online censorship and physical panoptic surveillance of "Internet cafes" frequenters.

[10] Available in Arabic at https://www.e.gov.kw/sites/kgoarabic/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf

[11] Available in Arabic at https://www.e.gov.kw/sites/kgoarabic/Forms/MediaLaw082016.pdf

3. Oman

Online activists and journalists have been widely targeted and prosecuted in Oman. Articles 17 and 19 of Oman's Cybercrime Law 12/2011[12] prosecute the use of the Internet and information communication technology (ICTs) to "publish or distribute or purchase or whatsoever" in ways that "violate public ethics" and "might prejudice the public order or religious values." These are penalised for a minimum of a month to a maximum of three years in prison. Article 18 penalises by imprisonment from one month to three years and fines any individual whose use of ICTs "threaten or extort a person to do or abstain from doing any act even if the doing or not doing of such an act is legal." Moreover, the penalisation is harsher (three to ten years in prison) when "the threat is to commit an offence or by attributing indecent acts affecting honour and superiority."

These Articles, due to their vague wording and loaded connotations, hinder human rights defenders' and activists' efforts to unveil corruption and injustice and can indeed be used to justify their prosecution. Unlike most Gulf countries, Oman does not have a cyberpolice department and cases are handled by the Internal Security Service (ISS).

Omani online activist **Hassan Al-Basham** passed away on 28 April 2018 while serving his prison sentence in the Samail Central Prison, to which he was admitted on 26 November 2017. Al-Basham relentlessly defended prisoners of conscience with his numerous writings. The case of Al-Basham demonstrated a number of violations to human rights, including the right to fair trial and prison conditions. The Omani Coalition for Human Rights urged the Omani authorities to investigate into the circumstances of Al-Basham's death.

On 17 September 2015, Al-Basham was first arrested by the ISS and appeared before the Special Division of the Omani Police in Sohar. He was released on 23 September 2015, and then arrested again two days later, on 25 September 2015, and subjected to a prolonged interrogation. On 08 February 2016, the Court of First Instance in Sohar sentenced Al-Basham to three years in prison on charges of "the use of the Internet in what might be prejudicial to religious values" as per Article 19 of the Cybercrime Law, also convicted for "insulting the Sultan" and fined. On 13 June 2016, the Court of Appeal in Sohar upheld the three-year prison sentence against Al-Basham while the fine for "insulting the Sultan" was overturned.

On 17 January 2017, the High Court revoked the three-year prison sentence against Al-Basham after examining his case due to his deteriorating health and the case was referred back to the Court of Appeal. The High Court took into account the fact that the request by the defense team to carry out a medical examination of the defendant was ignored during the trial. Nonetheless, on 19 November 2017, the Court of Appeal in Sohar again upheld the initial verdict of three years in prison to which he was initially sentenced by the Court of First Instance in Muscat. The Court of Appeal reportedly did not allow the defence team to present its evidence and medical reports.

[12] Official English version of the Law is available at the Omani Information Technology Authority website https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=54

A different tactic of repression that does not appear in the Cybercime Law was the travel ban imposed on human rights defender **Saeed Jadad**. At the security checkpoint in the airport, when planning to fly to Doha on 08 January 2017, Jadad found himself under an unannounced travel ban until 2099. The travel ban is another form of continued restrictions and targeting by the government violating Jadad's human rights due to his cyberactivism.

The history of the government's targeting Jadad dates back to 25 November 2015 when state security forces raided Jadad's home, detained and transferred him to Arzat prison in the city of Salalah. The arrest followed ratification by the Court of Appeal in Salalah on 18 November of the sentence issued by the Court of First Instance, to a one-year prison term and a fine of $2600. Jadad was convicted on charges of the "use of an information network (the Internet) in the dissemination of material that would prejudice public order," by the Court of First Instance on 07 April 2015. He served his sentence and was released on 26 August 2016.

Writer and activist **Hamood Al-Shukaily** was sentenced to a three-year prison sentence by the Court of First Instance in Muscat on 18 October 2016. It is important to note that the bail for Al-Shukaily to submit his appeal was as high as US$13,000. The charges were for "publishing a poem on Facebook," "incitement of protest," and "protesting *Azamn* arrests" in a Facebook post. On 18 January 2017, the Appeal Court in Muscat examined Al-Shukaily's case and ruled "to accept the appeal in form and reject it in substance in addition to stopping the prison sentence."

On 15 April 2017, Internet activist **Khalid Al-Ramadani** was arrested at the Omani-UAE border and transferred to the Special Division without access to his family or a lawyer. The arrest follows his criticism of government corruption on his personal Facebook account. **Ahmed Al-Bahri** was summoned by the ISS on 17 April for interrogation over posting criticism of the government on his personal Facebook account. Al-Bahri was one of the most notable leaders of a teacher's strike in 2011 and was sentenced to a one-year prison sentence for "disrupting public order" in 2014. This sentence was suspended by paying a fine of US$2600.

In an interview with women human rights defender **Habiba Al-Hinai**[13] on the conditions of civic space and status of human rights defenders, activists and civil society organisations and workers in Oman, she highlighted the extreme measures taken by the Omani government to intimidate and silence aforementioned groups. Such measures include monitoring and surveillance on WhatsApp communication and systemic prosecution for online content critical of the government and corruption which resulted in activists, workers and human rights defenders to completely stop posting online.

The CIVICUS Monitor Rating classifies Oman's civic space as "repressed."

[13] Al-Hinai was able to flee Oman before a travel ban is imposed on her and hence, was able to conduct this interview with CIVICUS.

4. Qatar

Combating cybercrime in the gulf is widely associated to the threat of the extension of human rights to the cyberspace. Accordingly, the criminalisation of the exercise of human rights was the pillar for the creation of cybercrime legislation. Similar to the case of Al-Shukaili in Oman, Qatari poet **Mohamed Al-Ajami** was sentenced to fifteen years for poem recitals that were online in 2011. The case of Al-Ajami is complicated as it criminalised Al-Ajami for the exercise of his freedom of speech and expression as the poems in question were critical of the ruling family and other rulers in the region, yet the publicity of the poems as online content worsened the sentence. Al-Ajami's initial verdict was a life sentence in 2012 which was appealed and lessened to fifteen years. Later, Al-Ajami was released on a pardon after spending almost five years in prison in 2016.

While the case of Al-Ajami was in court, Qatar issued its national cybercrime law in 2014[14], titled: "On suppression of electronic crimes." Article 2 of the law criminalises any unauthorised access to websites or information systems of any government body to a maximum of three years in prison and a fine of US$137,325. The penalty is harsher for access that implicates national security and economy.

Unlike the previously examined cybercrime laws, the Qatari legislation dedicates the second section of the Law (Articles 5 to 9) titled "criminal content," which details the different types of content to be prosecuted. First, Article 5 penalises the creation and administration of terrorist group's platforms on the Internet or other ICTs; as well as facilitating communication with these groups, their members or the propagating or financing their activities. Second, Article 6 criminalises the creation and administration of a website or uses ICTs to spread fake news that can compromise national security and public order, the penalty is the same as in Article 5. Complicit in Article 6 are those who share the fake news and they are penalised to a maximum of one year in prison and a fine of US$68,662. Article 8 follows the same fashion of employing vague terms to scrutinise content as it penalises any infringement upon morals and social mores to a maximum of three years in prison and a fine that does not exceed US$27,464.

Qatar has a limited number of documented cases given the extremely repressive measures taken by the government in order to silence dissident voices and annihilate the exercise of digital rights. Blogger and human rights defender **Sultan Al-Khalaifi** was held incommunicado on 02 March 2011 after he expressed on his blog his criticism of Qatar's censorship of books. **Najib Al-Nuaimi**, Al-Khalifi's lawyer at the time, explained that Al-Khalaifi has been harassed and arrested repeatedly for expressing his opinion and as such uncovers the defect in the legal code. The cybercrime legislation, however, came forth to strengthen this defect which augments prosecution of rights exercised online.

The CIVICUS Monitor Rating for Qatar is "repressed," that it is very limited and narrow space for activism.

[14] Available in Arabic at http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/100242/120183/F1232109237/100242.pdf

5. Saudi Arabia

Saudi Arabia is notorious for violation of user rights as warned by Human Rights Watch in a 2014 report which revealed that the government infected citizens' mobile phones with surveillance software, purchased from the Italian company Hacking Team, to invade their private communication by monitoring emails, text messaging services and calls.

Under the umbrella of its 2007 Anti-Cybercrime Law[15], advancing Anti-Terror Law, and judicial verdicts to restrict online freedoms of expression, opinion and thought, surveillance, violation of digital rights and arrests for online freedom of thought, expression and belief are justified. In essence, these legislations are manifest in the repressive measures undertaken by the Saudi government in prosecuting citizens for their different opinions expressed on religion, society and politics. In other cases, human rights defenders and activists have been under reprisal and targeting by the government, which was justified by their online activism or after they were accused of violations under the 16-Article Anti-Cybercrime Law.

Article 2 of the Law specifies that its purpose is to identify and combat cybercrimes in order to "protect public interest, morals, and common values." Article 6 is the most problematic article of the Law as it threatens online freedom of thought, expression and opinion as punishable offences. In this respect, Article 6 details that punishment for the "production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy" will lead to a five-year prison sentence and a fine of US$800,000 or either. The highest punishment in the Law is reflected in Article 7 which sets a prison sentence of no more than ten years and a fine of no more than US$1,333,375 or either for two cybercrimes: creation or circulation of terrorist organisations' websites, and "unlawful access" to data that should threaten national security or economy.

In this light, blogger **Raif Badawi** was sentenced to ten-years in prison followed by a ten-year travel ban and a fine of US $266,675 in 2012, in addition to publicly imposed one-thousand lashes, for creating a website entitled: the Liberal Saudi Network which engaged Saudi citizens in discussion on the social and political reforms.

Not only does the sentence Badawi received mirror the most severe punishment in the Law for establishing and supporting terrorist organisations, equating human rights activism and freedom of expression to terrorism was strengthened by issuing the Anti-Terror Law. The terms of Articles 2 and 6 of the Anti-Cybercrime Law were the main pillars of compiling the case to annihilate the activism of the group forming the **Saudi Civil and Political Rights Associations (ACPRA)**. Authorities have prosecuted ACPRA members for content posted and disseminated online on twitter and in messages. Moreover, ACPRA members were tried in unfair trials against the prerogatives in the Anti-Terror Law which deems all forms of expression and communication critical of the government as a terrorist threat.

[15] Official translation is retrieved from http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf.

Article 13 permits the confiscation of tools used to execute the named crimes, in addition to shutting down the venues temporarily or permanently where the so-called cybercrime took place. This Article is problematic as it justifies crackdowns on independent journalism or political activism, extending measures of censorship to the physical realm - and not just by limiting access to content which the government flags as a threat, as in the case of ACPRA. Cooperation between the Communications and Information Technology and security apparatus is sanctioned by the law while the Bureau of Investigation and Public Prosecution handles cybercrimes.

On 08 January 2017, **Essam Koshak** was detained by the Bureau of Investigation and Public Prosecution for supporting women's rights by tweeting using the (#IamMyOwnGuardian) hashtag. In August 2017, the government of Saudi Arabia further strengthened its grip on online content by creating a Department of Public Prosecution (DPP) that is tasked with monitoring and filtering social media to prosecute perpetrators of "hate speech.". The Spokesperson for the DPP, Attorney General Sheikh Saud Al-Mujab, named Twitter to be the primary platform of interest to combat the spread of "terrorist rhetoric" and "inciting violence" in light of his first case of prosecuting individuals for hate speech. Nonetheless, this invasive filtering and monitoring of social media has been dressed in combating terrorism and countering violence but the case of Abu Sin, a teenager, who was arrested for his YouTube videos that were deemed "unethical" and liable to prosecution under Article 6. Following the creation of the DPP, the Ministry of Interior requested Saudi Twitter users to report to the authorities content that is a threat to national unity and the state's reputation when they constitute acts of terrorism. Following this, 30 individuals of no political opposition or human rights activism history were arrested.

On 25 January 2018, authorities charged two human rights defenders, **Abdalla Madhi Al-Attawi** and **Mohammed Al-Otaibi** for their online activism and expression of solidarity for retweeting a tweet by a member of the ACPRA, signing and publishing online petitions and inciting public disorder. They were sentenced to seven and fourteen years respectively by the Specialised Criminal Court (SCC), which was created to prosecute terrorism cases. Following these developments, Koshak and **Issa Al-Nukhaifi**, who was arrested and charged for voicing his anti-war in Yemen activism online, have been prosecuted by the SCC as well.

Samar Badawi, **an** award-winning women human rights defender, was summoned by the Bureau of Investigation and Prosecution in Jeddah. On 15 February 2017, Badawi appeared before the Bureau to investigate one of her tweets related to her calls for civil and political rights, essentially the women's campaign against male guardians. Badawi has been under a travel ban since December 2014.

Internet activist **Naimah Al-Matrood** was arrested and detained by the Directorate of Public Investigation in April 2016. Al-Matrood was detained for a year before the first hearing of her trial on 13 April 2017, which started without the presence of her lawyer or family members. Al-Matrood was charged with participating in a number of anti-state demonstrations and rallies, being linked to a media cell, and violating public order by creating two social networking accounts on Twitter and Facebook advocating for the release of some detainees. On 10 November 2017, the SCC in Riyadh sentenced her to six years in prison followed by a six-year travel ban.

On the CIVICUS Monitor Rating , Saudi Arabia's rating is "closed" while on the Internet Freedom Score it scored 72/100. Violation of user rights is the most common restriction imposed by the government.

6. United Arab Emirates

The UAE is unconventional in its approach to cybercontrol and violation of user rights. The government does not shy away from veiling its Internet surveillance, monitoring, filtering and invasion of privacy of users, nationals and residents alike.

In 2015, the UAE announced, and started prosecuting, individuals for "swearing" and use of inappropriate language in personal communication which means that even private conversations over text messaging services like WhatsApp are monitored. In January 2018, a British resident in the UAE was sent to prison over a WhatsApp conversation which the recipient judged as "offensive." This tightening of civic space was voiced by the security apparatus in August 2011, exhibiting particular interest in social media platforms (Facebook and Twitter, namely) to monitor online activity, particularly any of interest in politics.

Although the first Cybercrime Law issued by the UAE was in 2006, the Federal Decree-Law (5) of 2012 abrogated the 2006[16] Law[17]. The UAE further modified Article 9 of the 2012 Law Combating Cybercrimes under the Federal-Decree Law (12) of 2016[18]. Article 29 criminalises online content that is deemed to infringe the "reputation, prestige or stature of the State or any of its institutions" or figures, even if this content is sarcastic. Article 38 further criminalises communication with any "organisations, institutions, authorities or any other entities… incorrect, inaccurate or misleading information that may damage the interest of the State or injures its reputation." In Article 29, the punishment is imprisonment and a fine that does not exceed US$272,245 while Article 38 sets the punishment as imprisonment only. Leaving the prison sentence undefined under the two Articles allows the authorities to maneuverer the term of detentions as long as it suits their political interests. Articles 29 to 38 criminalise digital content production which challenges the existing political, social and religious arrangements. Article 44 sums up crimes defined in Articles 29, 30 and 38 as state security crimes.

The reputation of the UAE on Twitter and Facebook is hence prime to respect for human rights and online freedom of thought and expression. **Obaid Al-Zaabi**, a human rights defender, was arrested for "setting up a Twitter account," "networking and dissemination of information that incite hatred," "accusing the State Security Apparatus of torture," and "accusing the rulers of UAE of injustice." Al-Zaabi was detained in December 2013 and only released in December 2017 even though the Federal Supreme Court of Abu Dhabi acquitted him of charges pressed against him on 26 May 2014.

[16] Unofficial translation of the Federal Law (2) of 2006 on the Prevention of Information Technology Crimes can be accessed at http://www.wipo.int/wipolex/en/text.jsp?file_id=316479.

[17] Official translation of the Federal-Decree Law (5) of 2012 on Combating Cybercrimes can be accessed at http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf.

[18] Text of Federal-Decree Law (15) of 2016 is available in Arabic at http://ejustice.gov.ae/downloads/latest_laws2016/unionlaw12_2016_5_2012.pdf.

Online activist **Osama Al-Najjar** was detained and tried on 17 March 2014 for protesting the prison conditions of his father **Hossain Al-Najjar** on Twitter. The charges were "offending and instigating hatred against the state" and "spreading lies," and he was sentenced to three years in prison and a fine of US$136,100. Al-Najjar was due to be released on 17 March 2017, yet he has still not been released. Human rights activist and academic, Dr. **Nasser Bin Ghaith** was arrested on 16 August 2015 and held incommunicado for posting online content deemed hostile to a foreign state and damages the UAE's reputation. On 16 January 2017, academic and activist Dr. **Abdulkhaleq Abdulla** was arrested by the state security apparatus for his tweets that called for freedom of expression.

Award-winning human rights defender **Ahmed Mansoor** was arrested from his home on 20 March 2017 and held incommunicado until his trial. The charges against Mansoor are for using social media platforms to attack the UAE's reputation, compromise national and social unity, and promoting sectarianism. Mansoor's case has been handled by UAE's Federal Public Prosecution for Cybercrimes.[19] This court was created on 13 March 2017 by a ministerial resolution, a week before Mansoor's arrest, tasked with prosecution of cases of online content that breaches public morality, calls for political activism, and critical of religions. Indeed breach of online privacy of users is commonplace in the UAE, yet the authorities have particularly targeted the devices of Mansoor and infected these with surveillance malware in 2012, purchased from the French company VUPEN, following his release in a separate case of five people sentenced for online activism in 2011, known as the UAE5. Previous attempts to compromise Mansoor's privacy in 2011 employed FinFisher's FinSpy spyware as well as Hacking Team's Remote Control System in 2012.

Similarly, two days after the creation of the Federal Public Prosecution for Cybercrimes, the Jordanian journalist **Tayseer Al-Najjar** was sentenced on 15 March 2017 to three years in prison and a fine of US$136,000 for a Facebook post which is ruled to "insult state's symbols." Under the text of Article 42, courts may order the deportation of foreigners charged with cybercrimes after serving their punishment.

UAE's Internet Freedom Score score is "not free," scoring 69/100, similar to Saudi Arabia, with violations of user rights being the most compromised aspect for a free Internet. The CIVICUS Monitor Rating categorises UAE's civic space as "closed."

IV. Cybercrime laws in neighbouring countries: Reinforcing repression and violations

1. Jordan

Jordan was one of the countries in the region which took the early venture of devising a cybercrime legal framework after the UAE and Saudi Arabia. Although the previous classifications do put Jordan in a position that is less repressive of civic and digital rights, it does not negate the national cybercrime legislation and prosecution which criminalises and penalises online freedoms.

[19] Cited also as Federal Public Prosecution for Information Technology Crimes.

The Jordanian Information Systems and Cybercrime Law of 2010[20] featured 17 articles which was later updated in 2015 to include one more. Article 11 criminalised sending, re-sending, publishing data or information over the web which vilify, slander or insult others. The penalty is no less than three-months in prison (no maximum limit to the sentence is mentioned) and a fine ranging from US$140 to $2812. Article 12(A) criminalises access to a "website" or information system that features content unauthorised by the government of concern to national security, the economy or foreign relations with a fine ranging from US$703 to $7037. The prison sentence is a minimum of four months and the law does not set a maximum prison sentence. Article 14 dictates the same penalty of the accused to those who "intentionally participate in, interfere or incite" the named crime. Article 15 follows the same vague and broad fabric for criminalisation as in other legislations in the region by specifying that prosecution of other crimes in other laws follows the set penalty.

On 03 August 2016, journalist and writer **Nahed Hattar** was charged for contempt of religion according to Article 105 of the Penal Code and the cybercrime law as the cartoon he shared was deemed "insulting." Beside the uproar the cartoon instigated, the authorities commented that such an act is not defined as freedom of expression but rather is a crime of contempt. Hattar was assassinated by extremists as he was going to stand trial for these charges on 25 September 2016.

The Combating Cybercrime Unit announced on 05 October 2016 the arrest of twelve individuals for instigating violence and sectarianism on social media and three for creating and publicising Whatsapp messages that offend and defame religions. Authorities reported that these individuals are linked to the assassination of Hattar but content of the messages was not announced. This not only is alarming for the unannounced details pertaining to the case but also the vulnerability of Jordanian citizens to state surveillance, violation of their privacy and personal communication and prosecution for the broadly defined "insulting" content.

Authorities continue to use the cybercrime law to prosecute more journalists. On 08 December 2016, journalist **Ziad Nussirat** was stopped by Jordanian General Security for Facebook posts deemed insulting of a citizen who filed a complaint against him. Furthermore, seven journalists were arrested and detained for uncovering corruption manifest in the increased wealth of Youssef Al-Isawi, the Secretary General for the Royal Hashemite Court[21] on 25 October 2017, after reporting on the possessions. Similar to the case of Nussirat, on 31 October 2017, the cartoonist **Emad Hajjaj** was summoned by the public prosecutor to investigate a cartoon published on his personal Facebook and Twitter accounts in which he depicts Jesus disowning Patriarch Theophilos III following his decision to sell property of the Orthodox Church of Jerusalem to Israel. Hajjaj risked trial under Jordan's restrictive Cybercrime and Press and Publication Laws, which if violated are penalised by a prison sentence.

[20] https://www.unodc.org/res/cld/document/information-systems-crime law_html/Jordan_Information_Systems_and_Cyber_Crime_Law.pdf

[21] The Royal Hashemite Court is the body which joins the King with the government, judiciary, legislature, the armed forces, and security services as the Court prepares and implements the King's national and international agenda.

By the end of 2017 and after this serious targeting of online freedom of press, thought and expression, the Jordanian government announced a proposal to further amend the cybercrime law. In this proposal, "hate speech" is stressed by adding an article which penalises and criminalises publishing and sharing content that is classified as "hate speech." The definition of course is broad enough to allow any form of freedom of expression to be attributed as hate speech. In this amendment to the law, hate speech is defined as: "any speech or action that would instigate sectarianism, religious, minority, ethnic or regional factionalism or discrimination between individuals and groups." The prison sentence for hate speech is no less than one year and no more than three years.[22]

Jordan's Internet Freedom Score ranking is 53/100, with the highest risk associated to violations of user rights, and it is classified as "obstructed" on the CIVICUS Monitor Rating .

2. Syria

The Syrian government has been skilled in circumventing online freedoms and digital rights since introducing the internet in 2000. From 2000-2010, Human Rights Watch documented the violations to human rights in a decade of Bashar Al-Assad's leadership. In their report, fifteen cases were examined, of which eleven were prosecuted for exercising their rights online. Some of these cases included prosecution for online right of expression and assembly, and journalism.

Muhannad and **Haytham Qutaysh**, and **Yahya Al-Aws** were arrested in 2002 for exchanging emails with a UAE newspaper to cover a story on the death of workers in Syria; they were charged for "using the Internet to publish 'false news' outside of Syria" prosecuted against the Press Law. **Mas`ud Hamed** uploaded photos documenting Syrian police brutality against a protest of Kurdish Syrian children in 2003, for which he was accused of attempting to "annex part of Syrian territory to another country."

Ali Zein Al-`Abideen Mej`an was detained for posting comments critical of Saudi Arabia in 2005, charged for an act "that spoil its ties with a foreign state." This is not different from the newly instated charges of "committing a hostile act against a neighbouring country" as mentioned above in the cybercrime laws and practices of Gulf countries.

Omar al-Abdullah, Tarek Ghorani, Maher Ibrahim Asper, Ayham Saqr, `Ulam Fakhour, Diab Siriya, and **Husam Melhem** were all detained in early 2006 as they exercised their digital right to assembly by forming a youth discussion group and their rights to freedom of expression by publishing articles critical of the government. Blogger **Tariq Biasi** was arrested in 2007 for "spreading false news" and "weakening national sentiment" after he posted comments critical of the government on a website. Consequently, as online platforms became more reliable as an alternative to shrinking civic space in Syria, the government blocked Facebook in 2007 to crack down on dissident voices.

[22] Draft is available in Arabic http://www.lob.jo/View_LawContent.aspx?ID=865.

Syria's current CIVICUS Monitor Rating is "closed" while its Internet Freedom Score score is 86/100 with the highest related to obstacles to access and violations of user rights. The Internet penetration rate in Syria is only at 31.9 percent. Limited Internet access is another violation of human rights as it risks the lives of more civilians who rely on the Internet to know how to evade attacks and remain connected to channels of assistance. The United Nations Human Rights Council released a non-binding resolution in 2016 which affirmed that network disruptions are a violation to human rights. The resolution does codify that barriers to access are a threat to human rights but also it becomes more critical in conflict-devastated regions where information is central to protect civilians, human rights defenders, bloggers and journalists. While the ban on Facebook and YouTube was lifted in August 2011, various forms of Internet circumvention have been put in place, culminating in formal prosecution by specialised courts. Syria becomes the second country in the region to establish public prosecution for cybercrimes after the UAE.

On 8 February 2012, Bashar Al-Assad issued Law 17 on Regulating Online Communications and Combating Cybercrimes[23]. The 36-article law subjugates online content to the mandates of the Media Regulation Law. Under this Cybercrime Law, Internet Service Providers (ISPs) are obligated to store user data, monitor and track traffic so that authorities are able to trace it back to the respective netizen under judicial scrutiny. Article 32 casts a wider web for prosecution as it is permitted by law to prosecute crimes under the penal code if it is done over the cyberspace.

The Cybercrime Police Department lists the same risks associated with cybercrimes as other governments in the region, namely, the threats to social stability and national economy. In the curriculum[24] developed to prepare and equip the prosecutors groomed to head Cybercrime Specialised Courts, online journalism is criminalised by the mandates of the Media Regulation Law. The Syrian authorities named a number of media outlets that are granted immunity from the Media Regulation Law based on a ruling that they are "professional media outlets" i.e. pro-government. These are "Al-Watan" online newspaper, "Zaman Al-Wasl", the "Legal Electronic Newspaper" (JLE) and "Thawra". In this regard, this scrutinises everyone who does not write for the named outlets, hence netizens, businesses, and religious leadership.

Article 12 of the Media Regulation Law criminalises freedom of expression, opinion, thought and press by prohibiting and criminalising production of content that can compromise national unity and security, defamatory to religions, content inciting sectarianism, and reporting on the military and armed forces unless authorised to carry-out this reporting. Article 95 complements these restrictions by ascribing "fake news" as a crime.

On 25 March 2018, the Syrian government approved by presidential decree the Anti-Cybercrime Law 9/2018, which is a refined version of its predecessor Cybercrime Law 17/2012. This amended law mandates the creation of specialised courts and delegates specialised jurists for the prosecution of cybercrimes in every governorate. The law specifically delegates the tasked public prosecution and specialised courts to judges who received respective training on prosecution of cybercrimes.

[23] The Law is available in Arabic at https://tinyurl.com/y8gwh6g4

[24] This toolkit was developed jointly by the Ministry of Communications and Technology and the Ministry of Justice. The first edition is accessible through this hyperlink https://tinyurl.com/yb53xedl

In July 2017, a consortium of the Syrian Ministries of Interior, Communications and Technology, and Justice and the Arab Academy for E-Business hosted a training for personnel who would be in charge of the detection and prosecution of cybercrimes. Particular aspects of the training included filtering online content, especially on social media, and collecting data stored on computers, information systems or storage devices to vindicate cases. This training was the government's stepping stone before the creation of specialised courts, which trained 65 judges and 27 personnel of the Cybercrime Police Department from Damascus and its suburbs and Quenitra and with plans to scale this training to other governorates. The 58 judges who have been appointed as specialised prosecutors for cybercrimes successfully completed the training before the decree of Law 9/2018. Although the number of assigned judges announced after the decree is less than the number announced in the Ministry of Interior's statement in July 2017, it is expected that the Syrian government will train more judges.

The Cybercrime Law 17/2012 scrutinises ISPs which do not comply with censorship imposed by the government on content deemed unlawful. Furthermore, Article 30 harshens the penalty for cybercrimes that allegedly affect the state or public stability. In light of this article and the practices by the Syrian government, which prosecutes journalists and human rights defenders routinely, the Law thus unfairly criminalises online freedom of expression and opinion; and the creation of specialised courts further threatens the status of online freedoms in Syria. Nonetheless, the amended Anti-Cybercrime Law retains complementarity with the Media Regulation Law 108/2011 and Counter-Terrorism Law 19/2012 which both criminalise freedom of expression, opinion and press under the pretexts of enticing violence and sectarianism or spreading fake news.

3. Lebanon

Lebanon did not draft a cybercrime legislation thus far. However, the Internal Security Forces (ISF) established in 2006 the Cybercrime and Intellectual Property Rights Bureau (CIPRB). The absence of any kind of legal framework which specifies the roles, duties and cases handled by the CIPRB left it to be a tool to criminalise the exercise of digital rights. Therefore, although the CIPRB announces on its website that it is concerned with prosecution of cybercrimes of fraud, piracy, blackmailing, etc. it has also been invested in the prosecution of online freedom of speech, expression and the press. The main legal backbone for this prosecution is defamation articles in the Penal Code which are vaguely defined.

The trend of prosecution has targeted netizens and journalists. In 2008, arrests for online freedom of thought and expression have been witnessed in Lebanon. Four students were detained, charged for defamation and use of insulting and offensive language on Facebook, and transferred to prison by upholding articles of the Penal Code. Activist **Michel Douaihy** was detained for nine days on 06 October 2015 for a Facebook post critical of government use of force against activists in detention compared to lighter treatment for people accused of violent acts. The charges for Douaihy's post were for inciting sectarianism and defamation. Journalist **Mohammad Nazzal** had a verdict of the same charges, was sentenced to six months in prison and a fine of US$633 for a Facebook status update. Civil society and journalism communities in Lebanon viewed this as an attack not only on freedom of press but also as reprisal on Nazzal for upholding integrity and principles of journalism.

On 06 December 2016, journalism student **Bassel al-Amin** was arrested and released six days later on bail pending the General Prosecutor's decision to press charges or drop his case because of a Facebook post. On 28 January 2017, **Hassan Saad** was detained to investigate a Facebook status he posted on 17 January 2017 critical of the government. Activist **Ahmad Amhaz** was arrested on 21 March 2017 for criticising the President, Prime Minister and Speaker of Parliament. After nine days of detention, Amhaz was released pending trial.

On 22 January 2018, activist **Ubada Youssef** was summoned and detained by the Lebanese Military Intelligence to investigate content he posted to Facebook from 2017. Youssef was released pending trial.

The most problematic aspect of Lebanon's governance of cyberspace is not just policing and prosecution of digital rights and freedoms, it is also that the government is actively engaged in violation of netizens' right to privacy. In 2015, Citizen Lab issued a report on the use of FinSpy spyware (the same spyware used to violate the rights of Emirati human rights defender Ahmed Mansoor) against netizens by two government bodies: the ISF and the General Directorate of General Security (GDGS). The spyware enabled the Internet Freedom Score, empowered by the specialised unit (CIPRB) to target bloggers, journalists and activists.

In January 2018, Lookout and Electronic Frontier Foundation reported[25] on a full-fledged cyberespionage campaign by the GDSG, naming the main agent behind this campaign "Dark Caracal." This campaign involves the launch of state-sponsored malware and spyware targeting mobile phones of targets in and beyond Lebanon. The report notes that Dark Caracal targets were "military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions" where the comprised data included "documents, call records, audio recordings, secure messaging client content, contact information, text messages, photos, and account data." The first time Dark Caracal was identified in 2016 for targeting activists and journalists critical of the government in Kazakhstan. Relatives, family members and lawyers of the targets were not spared and have been under surveillance as well.

Lebanon's Internet Freedom Score rating is 46/100 which classifies it as "partly free," but violations of user rights remain a problematic aspect. Lebanon is also classified as "obstructed" on the CIVICUS Monitor Rating. The gap between the two ratings can be best explained by the magnitude of repressive measures taken by the government to restrict the exercise of civic and digital rights. It is not as wide and repressive as in the UAE, Saudi Arabia and Syria, but similar to Jordan, where civic space is very limited but exists.

[25] The report can be accessed at https://www.lookout.com/info/ds-dark-caracal-ty

V. Conclusion

The surveyed countries' scores on the Internet Freedom Score and CIVICUS Monitor Rating ranged from the extremely autocratic to the more relatively open on civic space and respect for digital rights. The common and most essential problem across these countries is the violation of user rights and detentions for online freedom of expression, thought, opinion and press. These practices reverberate across the region forming an unspoken covenant that these violations of digital rights are lawful and permissible. The formal face for this covenant manifests in the regional concerted efforts to devise cybercrime laws which protect the repression of digital rights. In this light, it is not surprising to see how identical national cybercrime legislations are, knowing that essentially these copy the backbone legislations (cybercrime laws of the UAE, Saudi Arabia, Jordan and the ACCC). As a consequence, these two dynamics at play make reform efforts highly dependent on government efforts to amend the backbone legislation i.e. unlikely when reinforced by further crackdowns on digital rights in all the region.

Governments have galvanised the restrictive legislative frameworks by importing advanced surveillance technologies and software. Not only do these technologies violate netizens' right to privacy and pose a threat to their exercise of digital rights, they also normalise the persecution of human rights defenders, journalists and experts who are critical of this practice. Unveiling the repressive measures taken by governments to disallow any expression critical of corruption, violations of human rights and other injustices is key to supporting the activism of human rights defenders, bloggers and journalists. It is indispensable to highlight that only through observing human rights, digital rights, protecting online freedoms and ensuring Internet access are important for society at large. To this end, human rights defenders and activists are indeed protecting society and human rights through their activism and criticism of their respective governments.

Although prosecuting activists, human rights defenders and netizens for comments and content critical of other governments was not a very popular measure, it has now gained currency. This aggravates the repression of online freedoms. Just as how governments reinforce their repression and violations through regional cooperation, this practice normalises a government's prosecution of its own citizens for words that are critical of decisions that impact the status of human rights in the region. Hence, it appears that governments are now weary of the effect of the Internet as an alternative space not only in their countries but also in neighbouring countries, that indeed mutually support crackdowns on civic space and human rights. Though governments' scepticism could be traced back to the memory of the Arab Spring, human rights defenders have long fought and risked their lives before that time for the protection of human rights.

There are two trends at hand we anticipate to proliferate and feel compelled to warn against. First, legislation will introduce more restraints on online freedom of speech and expression under the label of combating "fake news." At the moment, the term has currency internationally, as well as having been repeatedly cited in the charges against human rights defenders and journalists, either for compromising national security or for threatening relations with neighbouring/foreign countries. Second, now that the UAE and Syria have developed two branches that are specialised in the prosecution of cybercrimes i.e. the police units and courts, other countries are likely to follow suit. In the same vein, countries picked up the creation of cybercrime police units/departments/directorates, specialised courts in cybercrime are likely to emerge in the near future. The status of these courts' respect for a fair judicial system by international standards is questionable for two reasons. First, the cybercrime laws they operate under are at their core criminalising digital rights. Second, the cases that have been referred to these courts thus far are of human rights defenders, academics, journalists and bloggers critical of the government. This makes it an arm for government reprisal as opposed to an independent body concerned with upholding the law.

VI. Recommendations

GCHR expresses its deep concern for the status of digital rights and civic space in the region in light of these developments.

Based on the present research and survey, GCHR makes recommendations to the following bodies:

To the European Union and member states:

1. Implement legislation placing controls on European cybersecurity firms to prevent them from exporting surveillance, filtering and monitoring technologies to repressive governments, which are used to restrict Internet freedom in the region and target activists and human rights defenders, thus contradicting Europe's commitment to the protection of human rights.

To governments in the Middle East:

2. Repeal repressive articles in cybercrime laws, press and media laws and the penal code which are used to prosecute the exercise of digital rights and freedom of press.

3. Rescind prison sentences for the exercise of digital rights by human rights defenders, bloggers, journalists and netizens critical of corruption, violations of human rights and wars.

To Internet Service Providers (ISPs) everywhere:

4. Develop a code of conduct and consumer protection regulations that observe human rights in business and does not infringe upon netizens' digital rights.

To the UN Human Rights Council:

5. Reintroduce the 2016 Resolution on *The promotion, protection and enjoyment of human rights on the Internet,* (32/13) as a binding resolution.

6. Urge governments in the region not to impose any form of network disruption, in order to protect human rights, especially in conflict-torn regions.